Attorney's Docket No. 1033048-000060

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Patent Application of	
Harold Poskanzer et al.	Group Art Unit: 2191
Application No.: 09/843,757	Examiner: KUO LIANG J TANG
Filed: April 30, 2001	Appeal No.:
For: AUTOMATED PROVISIONING OF COMPUTING NETWORKS USING A NETWORK DATABASE MODEL	

APPEAL BRIEF

Mail Stop APPEAL BRIEF - PATENTS
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Sir:

This appeal is from the decision of the Primary Examiner dated March 25, 2005, finally rejecting claims 1-27, which are reproduced as the Claims Appendix of this brief.

☐ A check covering the ☐ $250.00 (2402) ☐ $500.00 (1402) Government fee is filed herewith.

☒ Charge ☒ $250.00 (2402) ☐ $500.00 (1402) to Credit Card. Form PTO-2038 is attached.

The Commissioner is hereby authorized to charge any appropriate fees under 37 C.F.R. §§1.16, 1.17, and 1.21 that may be required by this paper, and to credit any overpayment, to Deposit Account No. 02-4800.

01/26/2006 JADD01 00000024 09843757
02 FC:2402 250.00 OP

Table of Contents

I. Real Party in Interest

The application is assigned to OpsWare, Inc., the successor in interest to Loudcloud, Inc.

II. Related Appeals and Interferences

There are no other appeals, interferences or judicial proceedings which may be related to, directly affect or be directly affected by, or have a bearing on the Board's decision in this appeal.

III. Status of Claims

The application contains claims 1-27, all of which are pending and stand finally rejected. This appeal is directed to claims 1-27.

IV. Status of Amendments

There were no amendments filed subsequent to the final Office Action.

V. Summary of Claimed Subject Matter

The claims are directed to the secure installation of software on a computer, e.g. a server, from a centralized location, via a network. An example of the type of system in which the claimed method can be implemented is illustrated in Figure 7 of the application. In this type of system, an agent 36 running on the computer securely receives a command to install software from a central communication gateway 38. In response thereto, the agent performs the necessary actions to obtain the software from a central file system 34, and install the software on the device where it resides. (Paragraphs 0049, 0051)

The exchange of messages between the agent and the communications gateway is depicted in Figure 10. The commands to perform the installation of the software are provided to the agent 36 by means of a command queue. Each queue

comprises a set of commands that are to be run by the agent in a specific order. Once a command queue has been created, a poke message 42 is sent from the gateway to the agent, informing the agent that there is a command to be run. The agent opens a new connection to the gateway and returns a response 44, inquiring about the command. By requiring the agent to open a new connection and request the command from the gateway, the possibility of spoofing by a third party is decreased. Upon receiving the inquiry 44 from the agent in response to a poke message, the gateway retrieves the first command in the queue, and provides it to the agent in a message 46, e.g. obtain and install a package at a designated address in the file system. The agent runs the command, and then reports back to the gateway with a result 48. If there is another command in the queue, it is retrieved by the gateway and forwarded to the agent. The process continues in this manner, until the end of the queue is reached, at which time the gateway responds to the agent's most recent inquiry with a message 50 that there is no command to be executed. (Paragraphs 0063-0066)

A locking mechanism is employed to ensure that agents are not overburdened. For instance, an agent queue locking device can be implemented on the network gateway, which stores a device identification number. This locking device prevents the gateway from attempting to send a second command queue to the device that is currently busy, whose identification number is stored by the locking device. Thus, attempts to execute a second queue on the device will be prevented, until the device is not busy and the locking signal has been removed from the device. (Paragraphs 0070-0076)

VI. Grounds of Rejection to be Reviewed on Appeal

The final Office Action presents two grounds of rejection for review on this appeal:

1. Claims 23-27 stand rejected under the second paragraph of 35 U.S.C. § 112, as lacking antecedent basis for certain claim terminology;

2. Claims 1-27 stand rejected under 35 U.S.C. § 103, as being unpatentable over the Smith et al patent (US 6,067,582) in view of the Borman et al patent (US 6,708,195).

It is noted that the final Office Action also contains a provisional rejection of claim 1 on the ground of obviousness-type double patenting, in view of claim 11 of copending Application No. 09/838,142. The Action states that the double patenting rejection will be withdrawn once the Examiner receives confirmation that claim 11 has been canceled from the copending application. That claim was canceled from the '142 application in an Amendment filed February 28, 2005. Accordingly, the provisional rejection is believed to have been rendered moot.

VII. Argument

A. Rejection Under 35 U.S.C. § 112

The rejection of claims 23-27 under the second paragraph of 35 U.S.C. § 112 asserts that claim 23 lacks antecedent basis for all but one of the steps that are positively recited therein. As an explanation for this ground of rejection, the Office Action states "[i]t could be any server or another agent or communication gateway or other device who can perform the action." (Office Action at page 4)

This statement does not establish a basis for the rejection of the claims under the second paragraph of 35 U.S.C. § 112. It does not identify any indefiniteness, per se, in the claims. Nor does it demonstrate a lack of antecedent basis for the cited claim terminology. Instead, it is directed to the *breadth* of the claim, namely that the recited steps could be carried out by any of a number of different devices, rather than being limited to a specific device. This is illustrated by the subsequent

statements in the Office Action that, for purposes of the prior art rejection, the examiner is interpreting the claim to recite "a server sending an acknowledgement...", "an agent determining whether the acknowledgement...", etc. (emphasis in original).

As stated in MPEP § 2173.04, "Breadth of a claim is not to be equated with indefiniteness." The fact that claim 23 may be broad enough to read on operations that could be carried out by different possible devices is not a basis to reject it as lacking antecedent basis for the terms in the claims. Since the claim is a method claim, Appellants should not be limited to specific structures for implementing the method, unless the prior art dictates otherwise.

The recited steps are clearly and definitively set forth in claim 23. The final Office Action has not demonstrated any indefiniteness in claim 23 that would support a rejection under the second paragraph of 35 U.S.C. § 112.

B. Rejection Under 35 U.S.C. § 103

The rejection of the claims alleges that the Smith patent discloses all of the claimed steps, with the exception of those pertaining to a locking signal or device. With respect to this locking feature, the Office Action relies upon the Borman patent at column 1, lines 22-41, and contends that it would be obvious to incorporate the disclosed subject matter into the system of the Smith patent.

As set forth in MPEP § 2143, there are three criteria that must be met to establish a *prima facie* case of obviousness:

> First, there must be some suggestion or motivation, either in the references themselves or in the knowledge generally available to one of ordinary skill in the art, to modify the reference or to combine reference teachings. Second, there must be a reasonable expectation of success. Finally, the prior art reference (or references when combined) must teach or suggest all the claim limitations.

The rejection fails to satisfy at least two of these criteria.

1. Teaching all claim limitations

The Smith patent is directed to the sales and distribution of software to end users. The process is initiated by the user, who provides a request for a software package, plus billing credentials, to an on-line "store". The software is downloaded and is "installed", by the user, sitting at the computer. The software to be installed contains an embedded agent that oversees the installation process. See, for example, the flow chart of Figure 2 and the description thereof that begins at column 6, line 21.

In contrast to this type of user-initiated operation, the claims recite a different approach in which the process is initiated from a location remote from the device on which the software is to be installed. For example, the first step of claims 1 and 23 is "sending a message to an agent residing on the hardware device informing the agent of a command to install software on the hardware device on which it resides." In connection with this subject matter, the Office Action refers to the Smith patent at column 4, lines 31-34. However, this portion of the patent does not disclose a message that is sent "to" an agent residing on the device where the installation is to take place. Rather, the patent discloses that a message is sent *from* the remote computer 10, i.e. the device on which the software is to be installed, to the content server 16.

Since the Smith patent discloses that the message is sent from the user's computer to the content server, it cannot be interpreted to disclose the second step recited in claim 1, namely "an agent verifying the validity of the message sent to it..." In the context of the Smith patent, since the message originated from the remote computer, there is no need for an agent residing on that computer to verify the validity of the message.

Similarly, with respect to claim 23, the Smith patent does not disclose the recited step "in response to said message, sending an acknowledgement to a communication network gateway." If the computer 10 sent the message in the first place, there is no need to send an acknowledgement to a gateway "in response to" that message.

In replying to Appellants' previous arguments pointing out these distinctions, the final Office Action states that the Smith patent discloses that a message is sent "to" an agent residing on the device where installation is to take place. In support of this statement, the Office Action refers to Figure 1 and the electrical connection 12 of the user's computer 10 to the network 14. However, this generic disclosure of two-way communications with the computer 10 does not suggest the particular subject matter recited in the claim. Specifically, claims 1 and 23 recite that the message sent to the agent residing on the hardware device "inform[s] the agent of a command to install software on the hardware device on which it resides". The Office Action does not identify where a message containing such information is sent to the user's computer 10. Nor does it show that an agent on that computer validates a message of this type with a communication gateway that sent it in the first place.

As such, the Office Action fails to establish that the criterion of a teaching in the references that suggests *all* of the claimed limitations.

2. Motivation to Combine References

Because of the differences identified above, as a general matter it would not be obvious to employ a locking signal in the system of the Smith patent. In the claimed arrangement, in which the installation of software on a device is initiated outside of the device itself, e.g. from a centralized location, there is always the possibility that two or more processes at the centralized location may attempt to install software on a given device at the same time. For this reason, a locking signal is employed at the central location, to prevent the two processes from competing for the same resources on the device.

In contrast, when the installation of software is initiated from the device on which it is to be installed, the same concerns do not exist. In other words, the device itself is not likely to initiate two separate requests to install software at the same time. Hence, there is no need to employ a locking signal in the context of the Smith patent.

Of particular significance, there is no teaching in the Borman patent which suggests the applicability of a lock signal to the system of the Smith patent. As purported motivation for combining the teachings of the two references, the Office

Action refers to the fact that the Borman patent relates to a multi-user environment, and is designed to control access to objects so that updates performed by one user are not overwritten by simultaneous updates by another user. There is no showing that these teachings apply to the system of the Smith patent. Specifically, there is no suggestion in the Smith patent that multiple users would be attempting to install software onto a given computer simultaneously. Rather, the Smith patent only suggests that a single user is operating the computer onto which software is being installed. The references to "multi-user environment" do not have any relation to the teachings of the Smith patent. Hence, the concerns expressed in the Borman patent do not apply in the system of the Smith patent.

For these reasons, it would not be obvious to employ a lock signal in the system of the Smith patent, either in view of the Borman patent, or otherwise. Hence, the references fail to meet the requirement of providing a teaching that would motivate a person of skill in the art to combine their disclosures in the manner set forth in the final Office Action.

C. Conclusion

The rejection under 35 U.S.C. § 112 has not identified any indefiniteness, per se, in claims 23-27. The rejection under 35 U.S.C. § 103 fails to meet at least two of the criteria for a *prima facie* case of obviousness. The rejections of the claims are not properly supported in the statute, and should be reversed.

VIII. Claims Appendix

See attached Claims Appendix for a copy of the claims involved in the appeal.

IX. Evidence Appendix

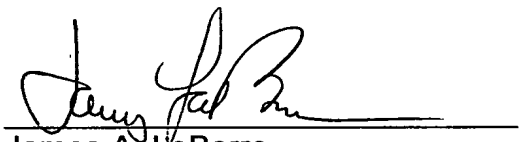
There is no Evidence Appendix for this Brief.

X. Related Proceedings Appendix

There is no Related Proceedings Appendix for this Brief.

Respectfully submitted,

Buchanan Ingersoll PC

Date January 25, 2006 By: 

James A. LaBarre
Registration No. 28,632

P.O. Box 1404
Alexandria, Virginia 22313-1404
(703) 836-6620

VIII. CLAIMS APPENDIX

The Appealed Claims

1. A method for installing software on a hardware device by an agent which resides on the hardware device comprising:

a communication network gateway sending a message to an agent residing on the hardware device informing the agent of a command to install software on the hardware device on which it resides;

an agent verifying the validity of the message sent to it with the communication network gateway;

the communication network gateway transmitting an indication regarding the validity of the command;

the agent receiving the command to install software on the hardware device if the indication transmitted from the gateway indicates that the command is valid;

the communication network gateway initiating a locking signal regarding using pre-determined resources of the hardware device to execute the command to install software on the hardware device;

the agent requesting files from a file server via the communication network gateway required for completion of the received installation command;

the file server sending the files required for completion of the received installation command to the agent via the communication network gateway;

the agent installing the files sent to it on the hardware device upon which it resides in response to the received installation command; and

the communication network gateway removing the locking signal associated with using the pre-determined resources of the hardware device to execute the command to install software in a hardware device after the files have been installed.

2. The method of claim 1, wherein the locking signal comprises a device resource locking signal that prevents the gateway from sending a second command relating to pre-determined resources of the hardware device in use by the agent installing software.

3. The system of claim 1, further comprising the communication gateway entering identification information of the hardware device and the pre-determined

resources of the hardware device required to execute the command to install software on the hardware device in a table within a system database.

4. The method of claim 3, wherein the table within the system database operates using uniqueness constraints for hardware device identification information contained therein.

5. The method of claim 4, wherein the locking signal comprises a uniqueness constraints signal.

6. The method of claim 4, wherein the table within the system database contains uniqueness constraints regarding resource identification information contained therein.

7. The method of claim 6, wherein the locking signal comprises a uniqueness constraint signal.

8. The method of claim 1, further comprising:
the agent installing the files according to an instruction set.

9. The method of claim 8, wherein the instruction set comprises the received installation command.

10. The method of claim 8, wherein the instruction set comprises a command queue.

11. The method of claim 8, wherein the instruction set resides in a network database.

12. The method of claim 8, wherein the instruction set resides in a network file server.

13. A method of controlling software commands executed on a hardware device by an agent, comprising the steps of:

the agent receiving a software command from a control network, which is part of a command queue;

the agent executing the software command on a hardware device;

determining resources on the hardware device currently in use;

preventing, by a locking device, a software command from the command queue from being executed upon the device if a resource it requires on the device for execution of the command is in use; and

repeating the steps of receiving, executing, and preventing by the agent until all commands of the command queue have been executed.

14. The method of claim 13, wherein the agent resides on the hardware device.

15. The method of claim 13, wherein the step of determining comprises determining all hardware device resources currently in use.

16. The method of claim 13, wherein the step of preventing comprises locking a group of resources on the hardware device.

17. The method of claim 16, wherein the step of preventing comprises locking all resources on the hardware device.

18. The method of claim 16, wherein the step of preventing comprises preventing the execution of software commands requiring one of the group of locked resources.

19. The method of claim 13, wherein the step of preventing comprises locking a single resource on the hardware device.

20. The method of claim 19, wherein the step of preventing comprises

preventing the execution of software commands requiring the single locked resource.

21. The method of claim 13, wherein the step of determining comprises verifying the presence of a resource identification number within a system database.

22. The method of claim 21, wherein each hardware device resource contained within the table of the system database is constrained by a uniqueness constraint.

23. A method for installing software on a hardware device by an agent which resides on the hardware device, comprising:

sending a message to an agent residing on the hardware device informing the agent of a command to install software on the hardware device on which it resides;

in response to said message, sending an acknowledgement to a communication network gateway;

determining whether the acknowledgement relates to a valid message, and if so transmitting a command from the gateway to the agent to install software on the hardware device;

initiating a locking signal regarding resources of the hardware device that are used to execute the command to install software on the hardware device;

providing files from a file server to the agent via the communication gateway;

installing the files on the hardware device by means of said agent; and

removing the locking signal after the files have been installed.

24. The method of claim 23, wherein the locking signal comprises a device resource locking signal that prevents the gateway from sending a second command relating to said resources of the hardware device.

25. The method of claim 23, wherein said locking signal is initiated and removed by said communication gateway.

26. The method of claim 23, wherein the locking signal comprises an entry in a table within a database that operates using uniqueness constraints for hardware device identification information contained therein.

27. The method of claim 26, wherein the locking signal comprises a uniqueness constraints signal.